UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,169	02/05/2004	Anat Bremler Bar	206,443	7298

7590 11/28/2005

JAY S. CINAMON, ABELMAN, FRAYNE & SCHWAB
150 East 42nd Street
New York, NY 10017

EXAMINER	
NGUYEN, THUONG	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 11/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/774,169	BAR ET AL.	
	Examiner	Art Unit	
	Thuong T. Nguyen	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-102* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-102* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/4/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to application 10/774,169 filed 10/18/00. Claims 1-102 are pending and represent method, apparatus and computer software product for detecting and protecting against worm traffic on a network.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Regarding claims 1, 29, 32, 35, 63, 66, 69, 97 and 100, the phrase "some of" renders the claim indefinite because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

4. Regarding claim 1, 35 and 69, the phrase "maybe" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

5. Regarding claim 1, 3, 35, 37, 69 and 71, the phrase "such that" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

6. Claims 9, 43 and 77 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The inventor fails to explain how to read or what is Time-To-Live.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-102 are rejected under 35 U.S.C. 102(e) as being anticipated by Afek Patent No. 2002/0083175 A1. Afek teaches the invention as claimed including method and apparatus for protecting against overload conditions on nodes of a distributed network (see abstract).

8. As to claim 1, Afek teaches a method for processing communication traffic, comprising:

monitoring the communication traffic that is directed to a group of addresses on a network (page 9, paragraph 240; Afek discloses that the method of monitored the communication links within the protected area of a distribution network);

determining respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group (page 15, paragraph 307; Afek discloses that the method of determined the access rate of the source IP addresses or any traffic classification parameters);

detecting a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, such that

the deviation is indicative that at least some of the communication traffic may be of malicious origin (page 16, paragraph 327; Afek discloses that the method of detected the access rate for the source IP addresses such as port numbers, protocol types for the malicious client); and

responsively to detecting the deviation, filtering the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin (page 11, paragraph 260; Afek discloses that the method of disabled and blocked the attack from the outside or inside of the protected area using the filtering technique).

9. As to claim 2, Afek teaches a method as recited in claim 1, wherein monitoring the communication traffic comprises selecting a subset of the group of the addresses to monitor responsively to the baseline characteristics (page 13, paragraph 295; Afek discloses that the method of monitored the IP addresses in the subsets of the network for any irregular/suspicious behavior).

10. As to claim 3, Afek teaches a method as recited in claim 2, wherein determining the respective baseline characteristics comprises determining respective amounts of the communication traffic that are directed to the addresses in the group, and wherein selecting the subset comprises selecting the addresses in the subset such that the addresses in the subset receive relatively small amounts of the communication traffic by comparison with other addresses in the group (page 13, paragraph 296; Afek discloses that the method of determined the volume of the overflow traffic for a period of time by comparing against the level of the central point).

11. As to claim 4, Afek teaches a method as recited in claim 1, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic (page 17, paragraph 333; Afek discloses that the method of distributed the communication for the TCP connection of the servers and clients).

12. As to claim 5, Afek teaches a method as recited in claim 1, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed (page 10, paragraph 245; Afek discloses that the method of distributed the sub-networks including dedicated networks, LANs and WANs).

13. As to claim 6, Afek teaches a method as recited in claim 1, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic (page 13, paragraph 294; Afek discloses that the method of distributed the source address, destination address, source port and destination port).

14. As to claim 7, Afek teaches a method as recited in claim 1, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group (page 17, paragraph 342; Afek discloses that the method of distributed the packet sizes, port numbers, the packets inter arrival times, and the ratio of the inbound and outbound traffic of the protocol for the source and server).

15. As to claim 8, Afek teaches a method as recited in claim 1, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic (page 10, paragraph 252; Afek discloses that the method of indicated the Network Operation for the routers and the systems).

16. As to claim 9, Afek teaches a method as recited in claim 8, wherein detecting the deviation comprises reading a Time-To-Live (TTL) field in headers of data packets sent to the addresses in the group, and detecting a change in values of the TTL field relative to the baseline characteristics (page 19, paragraph 387; Afek discloses that the method of periodicity for the distribution of packet inter-arrival times of a malicious daemon and the innocent source).

17. As to claim 10, Afek teaches a method as recited in claim 1, wherein detecting the deviation comprises detecting events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network (page 10, paragraph 256; Afek discloses that the method of detected the irregular traffic for the internal and external networks).

18. As to claim 11, Afek teaches a method as recited in claim 10, wherein detecting the events comprises detecting failures to establish a Transmission Control Protocol (TCP) connection (page 15, paragraph 310; Afek discloses that the method of monitored the TCP traffic for the system).

19. As to claim 12, Afek teaches a method as recited in claim 1, and comprising receiving packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to receiving the packets (page 15, paragraph 315; Afek discloses that the method of detected the malicious traffics based on the filter-rules for the IP addresses or subnetworks).

20. As to claim 13, Afek teaches a method as recited in claim 12, wherein receiving the packets comprises receiving Internet Control Message Protocol (ICMP) unreachable packets (page 17, paragraph 337; Afek discloses that the method of using the ICMP packets).

21. As to claim 14, Afek teaches a method as recited in claim 1, wherein monitoring the communication traffic comprises making a determination that one or more packets transmitted over the network are ill-formed, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to the ill-formed packets (page 10, paragraph 248; Afek discloses that the method of determined the malicious packets using filtering technique).

22. As to claim 15, Afek teaches a method as recited in claim 1, wherein detecting the deviation comprises incrementing a count of events that are indicative of the malicious origin of the communication traffic, and deciding whether to filter the communication traffic responsively to the count (page 12, paragraph 277; Afek discloses that the method of detected the attack volume for the maximum protection of the attacks).

23. As to claim 16, Afek teaches a method as recited in claim 15, wherein detecting the deviation comprises receiving data packets of potentially malicious origin, each data packet having a respective source address and destination address, and wherein incrementing the count comprises determining an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least

one data packet had the same respective source address and at least one data packet had the same respective destination address (page 10, paragraph 255; Afek discloses that the method of detected of the malicious packets for the IP address of the server for the network).

24. As to claim 17, Afek teaches a method as recited in claim 16, wherein determining the amount by which to increment the count comprises incrementing the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address (page 13, paragraph 290; Afek discloses that the method of determined the level of the victim traffic of the period of time).

25. As to claim 18, Afek teaches a method as recited in claim 1, wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein filtering the communication traffic comprises intercepting the communication traffic of the detected type (page 15, paragraph 308; Afek discloses that the method of detected the malicious client attacks for the victim available bandwidth).

26. As to claim 19, Afek teaches a method as recited in claim 18, wherein detecting the type comprises determining at least one of a communication protocol and a port that is characteristic of the communication traffic (page 16, paragraph 323; Afek discloses that the method of detected the communication protocol for the TCP packets).

27. As to claim 20, Afek teaches a method as recited in claim 18, wherein detecting the type comprises determining one or more source addresses of the communication

traffic that appears to be of the malicious origin, and intercepting the communication traffic sent from the one or more source addresses (page 12, paragraph 276; Afek discloses that the method of determined the malicious or overload traffic for the networks elements within the protected area).

28. As to claim 21, Afek teaches a method as recited in claim 1, wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein monitoring the communication traffic comprises collecting specific information relating to the traffic of the detected type (page 14, paragraph 297; Afek discloses that the method of detected the communication traffic for each potential victim traffic patterns of the packets/traffic filter).

29. As to claim 22, Afek teaches a method as recited in claim 21, wherein collecting the specific information comprises determining one or more source addresses of the traffic of the detected type (page 12, paragraph 279; Afek discloses that the method of determined the subset of the protected area).

30. As to claim 23, Afek teaches a method as recited in claim 1, wherein monitoring and filtering the communication traffic comprise monitoring and filtering the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area (page 11, paragraph 258; Afek discloses that the method of monitored the communication traffic for the public IP address for the protected area).

31. As to claim 24, Afek teaches a method as recited in claim 23, and comprising monitoring the communication traffic that is transmitted by computers in the protected

area so as to detect an infection of one or more of the computers by a malicious program (page 10, paragraph 253; Afek discloses that the method of monitored the communication traffic for the protected area for the victim outside the area).

32. As to claim 25, Afek teaches a method for processing communication traffic, comprising:

monitoring the communication traffic originating from a group of addresses and passing through a selected node on a network (page 9, paragraph 240; Afek discloses that the method of monitored the communication links within the protected area of a distribution network);

detecting a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses (page 13, paragraph 290; Afek discloses that the method of detected the malicious of the victim traffic); and

tracing a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious program is running (page 14, paragraph 305; Afek discloses that the method of identified the location of the port number and the source IP address).

33. As to claim 26, Afek teaches a method as recited in claim 25, wherein tracing the route comprises identifying a port of a switch on the network to which the computer is connected, and comprising disabling the identified port (page 15, paragraph 306; Afek discloses that the method of identified the malicious of the traffic).

34. As to claim 27, Afek teaches a method as recited in claim 25, wherein detecting the pattern comprises determining that the computer has transmitted packets to a large number of different destination addresses (page 17, paragraph 340; Afek discloses that the method of determined the IP address for the boarder router).

35. As to claim 28, Afek teaches a method as recited in claim 25, wherein detecting the pattern comprises detecting a large number of packets transmitted by the computer to a specified port (page 17, paragraph 343; Afek discloses that the method of detected the patterns for the traffic using the net flow).

36. As to claim 29, Afek teaches a method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection (page 11, paragraph 257; Afek discloses that the method of detected the possible attack in the protected area);

detecting an increase in a rate of arrival of the packets that are indicative of the communication failure (page 20, paragraph 392; Afek discloses that the method of detected the malicious packet based on the individual parameters of the clients); and

responsively to the increase, filtering the communication traffic so as to remove at least some of the communication traffic that is generated by the worm infection (page 18, paragraph 344; Afek discloses that the method of isolated the malicious traffic from the victim traffic by filtering packet from the routers and arriving from the host).

37. As to claim 30, Afek teaches a method as recited in claim 29, wherein monitoring the communication traffic comprises detecting Internet Control Message Protocol (ICMP) unreachable packets (page 17, paragraph 337; Afek discloses that the method of using the ICMP packets).

38. As to claim 31, Afek teaches a method as recited in claim 29, wherein monitoring the communication traffic comprises detecting failures to establish a Transmission Control Protocol (TCP) connection (page 15, paragraph 310; Afek discloses that the method of monitored the TCP traffic for the system).

39. As to claim 32, Afek teaches a method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect ill-formed packets (page 11, paragraph 257; Afek discloses that the method of detected the possible attack in the protected area);

making a determination, responsively to the ill-formed packets, that at least some of the communication traffic has been generated by a worm infection (page 13, paragraph 293; Afek discloses that the method of determined the malicious traffic by matching the filer rules for the packets originating from IP addresses or subnetworks); and

responsively to the determination, filtering the communication traffic so as to remove the at least some of the communication traffic that is generated by the worm infection (page 18, paragraph 344; Afek discloses that the method of isolated the

malicious traffic from the victim traffic by filtering packet from the routers and arriving from the host).

40. As to claim 33, Afek teaches a method as recited in claim 32, wherein the packets comprise a header specifying a communication protocol, and wherein monitoring the communication traffic comprises determining that the packets contain data that are incompatible with the specified communication protocol (page 14, paragraph 305; Afek discloses that the method of specified the port number of the IP address for the attack if the attack is not spoofed over many addresses).

41. As to claim 34, Afek teaches a method as recited in claim 32, wherein the packets comprise a header specifying a packet length, and wherein monitoring the communication traffic comprises determining that the packets contain an amount of data that is incompatible with the specified packet length (page 14, paragraph 301; Afek discloses that the method of determined the excessive traffic flows in the distributions reverse proxy connecting with the guard system).

42. As to claim 35, Afek teaches an apparatus for processing communication traffic, comprising:

a guard device, which is adapted to monitor the communication traffic that is directed to a group of addresses on a network (page 9, paragraph 240; Afek discloses that the apparatus of monitored the communication links within the protected area of a distribution network),

to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group (page 15, paragraph 307; Afek

discloses that the apparatus of determined the access rate of the source IP addresses or any traffic classification parameters),

to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, such that the deviation is indicative that at least some of the communication traffic may be of malicious origin (page 16, paragraph 327; Afek discloses that the apparatus of detected the access rate for the source IP addresses such as port numbers, protocol types for the malicious client), and

responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin (page 11, paragraph 260; Afek discloses that the apparatus of disabled and blocked the attack from the outside or inside of the protected area using the filtering technique).

43. As to claim 36, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to select a subset of the group of the addresses to monitor responsively to the baseline characteristics (page 13, paragraph 295; Afek discloses that the apparatus of monitored the IP addresses in the subsets of the network for any irregular/suspicious behavior).

44. As to claim 37, Afek teaches the apparatus as recited in claim 36, wherein the respective baseline characteristics are indicative of respective amounts of the communication traffic that are directed to the addresses in the group, and wherein the guard device is adapted to select the addresses in the subset such that the addresses

in the subset receive relatively small amounts of the communication traffic by comparison with other addresses in the group (page 13, paragraph 296; Afek discloses that the apparatus of determined the volume of the overflow traffic for a period of time by comparing against the level of the central point).

45. As to claim 38, Afek teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic (page 17, paragraph 333; Afek discloses that the apparatus of distributed the communication for the TCP connection of the servers and clients).

46. As to claim 39, Afek teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed (page 10, paragraph 245; Afek discloses that the apparatus of distributed the sub-networks including dedicated networks, LANs and WANs).

47. As to claim 40, Afek teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic (page 13, paragraph 294; Afek discloses that the apparatus of distributed the source address, destination address, source port and destination port).

48. As to claim 41, Afek teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group (page 17, paragraph 342; Afek discloses that the apparatus of distributed the packet sizes, port numbers, the packets inter arrival times, and the ratio of the inbound and outbound traffic of the protocol for the source and server).

49. As to claim 42, Afek teaches the apparatus as recited in claim 35, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic (page 10, paragraph 252; Afek discloses that the apparatus of indicated the Network Operation for the routers and the systems).

50. As to claim 43, Afek teaches the apparatus as recited in claim 42, wherein the guard device is adapted to read a Time-To-Live (TTL) field in headers of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems (page 19, paragraph 387; Afek discloses that the apparatus of periodicity for the distribution of packet inter-arrival times of a malicious daemon and the innocent source).

51. As to claim 44, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network (page 10, paragraph 256; Afek discloses that the apparatus of detected the irregular traffic for the internal and external networks).

52. As to claim 45, Afek teaches the apparatus as recited in claim 44, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection (page 15, paragraph 310; Afek discloses that the apparatus of monitored the TCP traffic for the system).

53. As to claim 46, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets (page 15, paragraph 315; Afek discloses that the apparatus of detected the malicious traffics based on the filter-rules for the IP addresses or subnetworks).

54. As to claim 47, Afek teaches the apparatus as recited in claim 46, wherein the packets comprises Internet Control Message Protocol (ICMP) unreachable packets (page 17, paragraph 337; Afek discloses that the apparatus of using the ICMP packets).

55. As to claim 48, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets (page 10, paragraph 248; Afek discloses that the apparatus of determined the malicious packets using filtering technique).

56. As to claim 49, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count (page 12, paragraph 277; Afek discloses that the apparatus of detected the attack volume for the maximum protection of the attacks).

57. As to claim 50, Afek teaches the apparatus as recited in claim 49, wherein the guard device is coupled to receive data packets of potentially malicious origin, each

data packet having a respective source address and destination address, and is adapted to determine an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address (page 10, paragraph 255; Afek discloses that the apparatus of detected of the malicious packets for the IP address of the server for the network).

58. As to claim 51, Afek teaches the apparatus as recited in claim 40, wherein the guard device is adapted to increment the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address (page 13, paragraph 290; Afek discloses that the apparatus of determined the level of the victim traffic of the period of time).

59. As to claim 52, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type (page 15, paragraph 308; Afek discloses that the apparatus of detected the malicious client attacks for the victim available bandwidth).

60. As to claim 53, Afek teaches the apparatus as recited in claim 52, wherein the type of the communication traffic that appears to be of the malicious origin is

characterized by at least one of a communication protocol and a port (page 16, paragraph 323; Afek discloses that the apparatus of detected the communication protocol for the TCP packets).

61. As to claim 54, Afek teaches the apparatus as recited in claim 52, wherein the guard device is adapted to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses (page 12, paragraph 276; Afek discloses that the apparatus of determined the malicious or overload traffic for the networks elements within the protected area).

62. As to claim 55, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to monitor the communication traffic so as to collect specific information relating to the traffic of the detected type (page 14, paragraph 297; Afek discloses that the apparatus of detected the communication traffic for each potential victim traffic patterns of the packets/traffic filter).

63. As to claim 56, Afek teaches the apparatus as recited in claim 55, wherein the specific information comprises one or more source addresses of the traffic of the detected type (page 12, paragraph 279; Afek discloses that the apparatus of determined the subset of the protected area).

64. As to claim 57, Afek teaches the apparatus as recited in claim 35, wherein the guard device is adapted to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses

so as to exclude the communication traffic from the area (page 11, paragraph 258; Afek discloses that the apparatus of monitored the communication traffic for the public IP address for the protected area).

65. As to claim 58, Afek teaches the apparatus as recited in claim 57, wherein the guard device is adapted to monitor the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program (page 10, paragraph 253; Afek discloses that the apparatus of monitored the communication traffic for the protected area for the victim outside the area).

66. As to claim 59, Afek teaches the apparatus for processing communication traffic, comprising:

a guard device, which is adapted to monitor the communication traffic originating from a group of addresses and passing through a selected node on a network (page 9, paragraph 240; Afek discloses that the apparatus of monitored the communication links within the protected area of a distribution network),

to detect a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses (page 13, paragraph 290; Afek discloses that the apparatus of detected the malicious of the victim traffic), and

to trace a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious

program is running (page 14, paragraph 305; Afek discloses that the apparatus of identified the location of the port number and the source IP address).

67. As to claim 60, Afek teaches the apparatus as recited in claim 59, wherein the guard device is adapted to identify a port of a switch on the network to which the computer is connected, and to instruct the switch to disable the identified port (page 15, paragraph 306; Afek discloses that the apparatus of identified the malicious of the traffic).

68. As to claim 61, Afek teaches the apparatus as recited in claim 59, wherein the guard device is adapted to detect the pattern by determining that the computer has transmitted packets to a large number of different destination addresses (page 17, paragraph 340; Afek discloses that the apparatus of determined the IP address for the boarder router).

69. As to claim 62, Afek teaches the apparatus as recited in claim 59, wherein the guard device is adapted to detect the pattern by detecting a large number of packets transmitted by the computer to a specified port (page 17, paragraph 343; Afek discloses that the apparatus of detected the patterns for the traffic using the net flow).

70. As to claim 63, Afek teaches the apparatus for processing communication traffic, comprising:

a guard device, which is adapted to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection (page 11, paragraph 257; Afek discloses that the apparatus of detected the possible attack in the protected area),

to detect an increase in a rate of arrival of the packets that are indicative of the communication failure (page 20, paragraph 392; Afek discloses that the apparatus of detected the malicious packet based on the individual parameters of the clients), and

responsively to the increase, to filter the communication traffic so as to remove at least some of the communication traffic that is generated by the worm infection (page 18, paragraph 344; Afek discloses that the apparatus of isolated the malicious traffic from the victim traffic by filtering packet from the routers and arriving from the host).

71. As to claim 64, Afek teaches the apparatus as recited in claim 63, wherein the guard device is adapted to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure (page 17, paragraph 337; Afek discloses that the apparatus of using the ICMP packets).

72. As to claim 65, Afek teaches the apparatus as recited in claim 63, wherein the guard device is adapted to detect failures to establish a Transmission Control Protocol (TCP) connection (page 15, paragraph 310; Afek discloses that the apparatus of monitored the TCP traffic for the system).

73. As to claim 66, Afek teaches the apparatus for processing communication traffic, comprising:

a guard device, which is adapted to monitor the communication traffic on a network so as to detect ill-formed packets (page 11, paragraph 257; Afek discloses that the apparatus of detected the possible attack in the protected area),

to make a determination, responsively to the ill-formed packets, that at least some of the communication traffic has been generated by a worm infection (page 13,

paragraph 293; Afek discloses that the apparatus of determined the malicious traffic by matching the filer rules for the packets originating from IP addresses or subnetworks), and

responsively to the determination, to filter the communication traffic so as to remove the at least some of the communication traffic that is generated by the worm infection (page 13, paragraph 293; Afek discloses that the apparatus of determined the malicious traffic by matching the filer rules for the packets originating from IP addresses or subnetworks).

74. As to claim 67, Afek teaches the apparatus as recited in claim 66, wherein the packets comprise a header specifying a communication protocol, and wherein the guard device is adapted to detect that the packets contain data that are incompatible with the specified communication protocol (page 14, paragraph 305; Afek discloses that the apparatus of specified the port number of the IP address for the attack if the attack is not spoofed over many addresses).

75. As to claim 68, Afek teaches the apparatus as recited in claim 66, wherein the packets comprise a header specifying a packet length, and wherein the guard device is adapted to detect that the packets contain an amount of data that is incompatible with the specified packet length (page 14, paragraph 301; Afek discloses that the apparatus of determined the excessive traffic flows in the distributions reverse proxy connecting with the guard system).

76. As to claim 69, Afek teaches a computer software product, comprising:

monitor communication traffic that is directed to a group of addresses on a network (page 9, paragraph 240; Afek discloses that the computer software product of monitored the communication links within the protected area of a distribution network),

to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group (page 15, paragraph 307; Afek discloses that the computer software product of determined the access rate of the source IP addresses or any traffic classification parameters),

to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, such that the deviation is indicative that at least some of the communication traffic may be of malicious origin (page 16, paragraph 327; Afek discloses that the computer software product of detected the access rate for the source IP addresses such as port numbers, protocol types for the malicious client), and

responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin (page 11, paragraph 260; Afek discloses that the computer software product of disabled and blocked the attack from the outside or inside of the protected area using the filtering technique).

77. As to claim 70, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to select a subset of the group of the addresses to monitor responsively to the baseline characteristics (page 13, paragraph 295; Afek

discloses that the computer software product of monitored the IP addresses in the subsets of the network for any irregular/suspicious behavior).

78. As to claim 71, Afek teaches the product as recited in claim 70, wherein the respective baseline characteristics are indicative of respective amounts of the communication traffic that are directed to the addresses in the group, and wherein the instructions cause the computer to select the addresses in the subset such that the addresses in the subset receive relatively small amounts of the communication traffic by comparison with other addresses in the group (page 13, paragraph 296; Afek discloses that the computer software product of determined the volume of the overflow traffic for a period of time by comparing against the level of the central point).

79. As to claim 72, Afek teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic (page 17, paragraph 333; Afek discloses that the computer software product of distributed the communication for the TCP connection of the servers and clients).

80. As to claim 73, Afek teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed (page 10, paragraph 245; Afek discloses that the computer software product of distributed the sub-networks including dedicated networks, LANs and WANs).

81. As to claim 74, Afek teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of source addresses of the

communication traffic (page 13, paragraph 294; Afek discloses that the computer software product of distributed the source address, destination address, source port and destination port).

82. As to claim 75, Afek teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group (page 17, paragraph 342; Afek discloses that the computer software product of distributed the packet sizes, port numbers, the packets inter arrival times, and the ratio of the inbound and outbound traffic of the protocol for the source and server).

83. As to claim 76, Afek teaches the product as recited in claim 69, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic (page 10, paragraph 252; Afek discloses that the computer software product of indicated the Network Operation for the routers and the systems).

84. As to claim 77, Afek teaches the product as recited in claim 76, wherein instructions cause the computer to read a Time-To-Live (TTL) field in headers of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems (page 19, paragraph 387; Afek discloses that the computer software product of periodicity for the distribution of packet inter-arrival times of a malicious daemon and the innocent source).

85. As to claim 78, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network (page 10, paragraph 256; Afek discloses that the computer software product of detected the irregular traffic for the internal and external networks).

86. As to claim 79, Afek teaches the product as recited in claim 78, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection (page 15, paragraph 310; Afek discloses that the computer software product of monitored the TCP traffic for the system).

87. As to claim 80, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets (page 15, paragraph 315; Afek discloses that the computer software product of detected the malicious traffics based on the filter-rules for the IP addresses or subnetworks).

88. As to claim 81, Afek teaches the product as recited in claim 80, wherein the packets comprises Internet Control Message Protocol (ICMP) unreachable packets (page 17, paragraph 337; Afek discloses that the computer software product of using the ICMP packets).

89. As to claim 82, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to make a determination that one or more packets

transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets (page 10, paragraph 248; Afek discloses that the computer software product of determined the malicious packets using filtering technique).

90. As to claim 83, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count (page 12, paragraph 277; Afek discloses that the computer software product of detected the attack volume for the maximum protection of the attacks).

91. As to claim 84, Afek teaches the product as recited in claim 83, wherein when the computer is coupled to receive data packets of potentially malicious origin, each data packet having a respective source address and destination address, the instructions cause the computer to determine an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address (page 10, paragraph 255; Afek discloses that the computer software product of detected of the malicious packets for the IP address of the server for the network).

92. As to claim 85, Afek teaches the product as recited in claim 84, wherein the instructions cause the computer to increment the count only if none of the data packets

received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address (page 13, paragraph 290; Afek discloses that the computer software product of determined the level of the victim traffic of the period of time).

93. As to claim 86, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type (page 15, paragraph 308; Afek discloses that the computer software product of detected the malicious client attacks for the victim available bandwidth).

94. As to claim 87, Afek teaches the product as recited in claim 86, wherein the type of the communication traffic that appears to be of the malicious origin is characterized by at least one of a communication protocol and a port (page 16, paragraph 323; Afek discloses that the computer software product of detected the communication protocol for the TCP packets).

95. As to claim 88, Afek teaches the product as recited in claim 86, wherein the instructions cause the computer to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses (page 12, paragraph 276; Afek discloses that the computer software product of determined the malicious or overload traffic for the networks elements within the protected area).

96. As to claim 89, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to monitor the communication traffic so as to collect specific information relating to the traffic of the detected type (page 14, paragraph 297; Afek discloses that the computer software product of detected the communication traffic for each potential victim traffic patterns of the packets/traffic filter).

97. As to claim 90, Afek teaches the product as recited in claim 89, wherein the specific information comprises one or more source addresses of the traffic of the detected type (page 12, paragraph 279; Afek discloses that the computer software product of determined the subset of the protected area).

98. As to claim 91, Afek teaches the product as recited in claim 69, wherein the instructions cause the computer to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area (page 11, paragraph 258; Afek discloses that the computer software product of monitored the communication traffic for the public IP address for the protected area).

99. As to claim 92, Afek teaches the product as recited in claim 91, wherein the instructions cause the computer to monitor the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program (page 10, paragraph 253; Afek discloses that the computer software product of monitored the communication traffic for the protected area for the victim outside the area).

100. As to claim 93, Afek teaches the computer software product, comprising:

to monitor the communication traffic originating from a group of addresses and passing through a selected node on a network (page 9, paragraph 240; Afek discloses that the computer software product of monitored the communication links within the protected area of a distribution network),

to detect a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses (page 13, paragraph 290; Afek discloses that the computer software product of detected the malicious of the victim traffic), and

to trace a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious program is running (page 14, paragraph 305; Afek discloses that the computer software product of identified the location of the port number and the source IP address).

101. As to claim 94, Afek teaches the product as recited in claim 93, wherein the instructions cause the computer to identify a port of a switch on the network to which the computer is connected, and to instruct the switch to disable the identified port (page 15, paragraph 306; Afek discloses that the computer software product of identified the malicious of the traffic).

102. As to claim 95, Afek teaches the product as recited in claim 93, wherein the instructions cause the computer to detect the pattern by determining that the computer has transmitted packets to a large number of different destination addresses (page 17,

paragraph 340; Afek discloses that the computer software product of determined the IP address for the boarder router).

103. As to claim 96, Afek teaches the product as recited in claim 93, wherein the instructions cause the computer to detect the pattern by detecting a large number of packets transmitted by the computer to a specified port (page 17, paragraph 343; Afek discloses that the computer software product of detected the patterns for the traffic using the net flow).

104. As to claim 97, Afek teaches the computer software product, comprising:

to monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection (page 11, paragraph 257; Afek discloses that the computer software product of detected the possible attack in the protected area),

to detect an increase in a rate of arrival of the packets that are indicative of the communication failure (page 20, paragraph 392; Afek discloses that the computer software product of detected the malicious packet based on the individual parameters of the clients), and

responsively to the increase, to filter the communication traffic so as to remove at least some of the communication traffic that is generated by the worm infection (page 18, paragraph 344; Afek discloses that the computer software product of isolated the malicious traffic from the victim traffic by filtering packet from the routers and arriving from the host).

105. As to claim 98, Afek teaches the product as recited in claim 97, wherein the instructions cause the computer to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure (page 17, paragraph 337; Afek discloses that the computer software product of using the ICMP packets).

106. As to claim 99, Afek teaches the product as recited in claim 97, wherein the instructions cause the computer to detect failures to establish a Transmission Control Protocol (TCP) connection (page 15, paragraph 310; Afek discloses that the computer software product of monitored the TCP traffic for the system).

107. As to claim 100, Afek teaches the computer software product, comprising:

to monitor the communication traffic on a network so as to detect ill-formed packets (page 11, paragraph 257; Afek discloses that the computer software product of detected the possible attack in the protected area),

to make a determination, responsively to the ill-formed packets, that at least some of the communication traffic has been generated by a worm infection (page 13, paragraph 293; Afek discloses that the computer software product of determined the malicious traffic by matching the filer rules for the packets originating from IP addresses or subnetworks), and

responsively to the determination, to filter the communication traffic so as to remove the at least some of the communication traffic that is generated by the worm infection (page 13, paragraph 293; Afek discloses that the computer software product of determined the malicious traffic by matching the filer rules for the packets originating from IP addresses or subnetworks).

108. As to claim 101, Afek teaches the product as recited in claim 100, wherein the packets comprise a header specifying a communication protocol, and wherein the instructions cause the computer to detect that the packets contain data that are incompatible with the specified communication protocol (page 14, paragraph 305; Afek discloses that the computer software product of specified the port number of the IP address for the attack if the attack is not spoofed over many addresses).

109. As to claim 102, Afek teaches the product as recited in claim 100, wherein the packets comprise a header specifying a packet length, and wherein the instructions cause the computer to detect that the packets contain an amount of data that is incompatible with the specified packet length (page 14, paragraph 301; Afek discloses that the computer software product of determined the excessive traffic flows in the distributions reverse proxy connecting with the guard system).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thuong T. Nguyen whose telephone number is 571-272-3864. The examiner can normally be reached on 7:30AM-4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Thuong T Nguyen
Patent Examiner/Art Unit 2155

SALEH NAJJAR
SUPERVISORY PATENT EXAMINER